

PREPARED STATEMENT OF
ATTORNEY GENERAL CHARLIE CRIST
STATE OF FLORIDA

Before the

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON ENERGY AND COMMERCE
U.S. HOUSE OF REPRESENTATIVES

on

Internet Data Brokers and Pretexting: Who has Access to Your Private Records?

June 22, 2006

Chairman Whitfield, Ranking Member Stupak, members of the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, U.S. House of Representatives, I am Julia Harris, and on behalf of Attorney General Charlie Crist of the State of Florida, I thank you for the opportunity to appear before the Subcommittee to address its concerns which resulted in this hearing on Internet Data Brokers and Pretexting: Who has Access to Your Private Records?

I. Background

I am a Senior Assistant Attorney General with the State of Florida Office of the Attorney General, Economic Crimes Division.¹ I am the attorney who filed litigation on behalf of Attorney General Charlie Crist against Global Information Group, Inc. on February 23, 2006 in state court in Tampa, Florida for unlawfully obtaining and selling confidential telephone records without the knowledge of the consumers whose records were being sold.

II. Attorney General's Litigation Against Data Brokers

A. *State of Florida vs. 1st Source Information Specialists, Inc., et al*

Attorney General Crist filed Florida's first lawsuit against data brokers trafficking in phone records on January 24, 2006 against 1st Source Information Specialists, Inc. et al, which conducted its Ft. Lauderdale, Florida based operations, in part, through the websites: locatecell.com, celltolls.com. datafind.org and peoplesearchamerica.com.² These websites

¹ The views expressed in this statement represent the views of the Attorney General. My oral testimony and responses to questions reflect my own views and do not necessarily represent the views of the Office of the Attorney General.

² *State of Florida v. 1st Source Information Specialists, Inc. et al*, Case No.:06-CA-234, Leon County Circuit Court (Honorable Lindy Lewis, Circuit Judge). Steven Schwartz and Kenneth Gorman were also named as defendants in the action. A default has been entered against defendant Gorman.

advertised the sale of telephone records, including records of outgoing calls from landline and wireless phones, and accepted orders for telephone records from any person with internet access, with no questions asked. In fulfilling orders, 1st Source unlawfully obtained and sold telephone records without consumer consent.

Through investigative coordination with the Florida Public Service Commission (the state regulatory authority responsible for telecommunications providers), a State investigator ordered telephone records on a Florida telephone number through the internet website peoplesearchamerica.com with a credit card payment of \$185.00. Before 24 hours had elapsed, the telephone records of the desired telephone number were e-mailed to the purchaser. The person subscribing to the telephone number that was the subject of the purchase did not consent to the sale of records.

B. *State of Florida vs. Global Information Group, Inc., et al.*

The Attorney General sued Global Information Group, Inc. (“Global”), Laurie Misner⁷, Global’s President and majority shareholder, and Edward Herzog⁸, a shareholder, officer, and owner of the predecessor business, alleging that the Global defendants violated

The 1st Source Complaint is available at:
[http://myfloridalegal.com/webfiles.nsf/WF/MRAY-6L8KGC/\\$file/1stSource_Complaint.pdf](http://myfloridalegal.com/webfiles.nsf/WF/MRAY-6L8KGC/$file/1stSource_Complaint.pdf)

The Subcommittee on Oversight and Investigations requested and subpoenaed documents from Steven Schwartz and subsequently subpoenaed Mr. Schwartz’s appearance before the Subcommittee on June 21, 2006.

⁷ Laurie Misner purchased the business known as Global Information Group, Inc. from Edward Herzog in 2005, with Mr. Herzog remaining an integral part of the business. The Subcommittee on Oversight and Investigations requested information from Laurie Misner as part of its investigation. Representatives from the Subcommittee have represented that Ms. Misner will appear before the Subcommittee for testimony on June 21, 2006.

⁸ Representatives from the Subcommittee have represented that Mr. Herzog has been subpoenaed to appear before the Subcommittee for testimony on June 21, 2006.

Florida's Deceptive and Unfair Trade Practices Act⁹, including the Criminal Use of Personal Identification Information law¹⁰ as per se violations¹¹ of the Deceptive and Unfair Trade Practices Act.¹² The Attorney General alleged that Global obtained information by impersonating either customers or telephone company employees in order to obtain consumers' personal calling information. Exhibits "C" and "D" to the complaint append transcripts of calls logged to customer service centers, one of which used the ploy of assisting a voice-impaired customer as a means to manipulate the release of customer information. In particular, the complaint alleged that Global made over 5,100 calls from its Florida-based operations to a telephone company customer service number in a span of just over a month period. Thousands of other calls originating from telephone numbers to which Global subscribed were made to several telephone companies' toll free customer service numbers.¹³ Global represented itself as "a leading provider of skip tracing services, asset recovery and information research" and that it

⁹ Chapter 501, Part II, Florida Statutes (2005).

¹⁰ Section 817.568(2), Florida Statutes (2005)

¹¹ Section 501.201(3)(c), Florida Statutes (2005)

¹² The Complaint is available at: [http://myfloridalegal.com/webfiles.nsf/WF/MRAY-6M9RY3/\\$file/Global_Complaint.pdf](http://myfloridalegal.com/webfiles.nsf/WF/MRAY-6M9RY3/$file/Global_Complaint.pdf)

Press Release: Crist Charges Second Data Broker Over Sale of Phone Records - Global Information Group, Inc. Provided Private Telephone Records To Third Parties
http://myfloridalegal.com/_852562220065EE67.nsf/0/5DEE071447E329878525711F0051E195?Open&Highlight=0,global

¹³ In addition to Florida's action, Global has been sued by three telecommunications providers (Verizon Wireless, T-Mobile, and Cingular Wireless) as well as by an individual, Charles Jones, Sr., in Jones v. Global Information Group, Inc., et al in Indiana Federal court. The providers have all obtained injunctions to date, specific to their entities. The private cause of action is active and ongoing.

“serves principally financial institutions, providing them with information necessary for recovery of lost assets from delinquent debtors.”¹⁴

On April 12, 2006, the Attorney General obtained a Consent Judgment and Permanent Injunction against Global, and defendants Misner and Herzog, individually.¹⁵

The Attorney General’s litigation constituted civil enforcement, with the judgment providing for monetary relief of \$250,000 and potential penalties of \$2.5 million against an offending individual defendant if certain conditions are met. The Attorney General required broad permanent injunctive relief due to the range of Global’s conduct involving pretexting. In addition to procuring a variety of telephone records, Global marketed, offered and/or provided services facilitated through pretexting which included:

skip tracing	utility searches
employment	unemployment
p.o. box / private mail boxes	social security benefits
disability benefits	welfare benefits
child support	social security number trace
school class schedules	cell phone triangulation

with performance of such services without the consent of the individual about whom an investigation was instituted. As a result of the terms required by the Attorney General’s

¹⁴ *Cellco Partnership d/b/a Verizon Wireless v. Global Information Group, Inc, et al*; Case No.: 05-09757; Hillsborough County Circuit Court; Motion to Dismiss Complaint Against Edward Herzog, filed Dec. 2, 2005

¹⁵ The Consent Judgment and Permanent Injunction is available at:
[http://myfloridalegal.com/webfiles.nsf/WF/MRAY-6NSLD8/\\$file/Global_Settlement.pdf](http://myfloridalegal.com/webfiles.nsf/WF/MRAY-6NSLD8/$file/Global_Settlement.pdf)

Press Release: Crist: Judgment to End Data Broker’s Business
http://myfloridalegal.com/_852562220065EE67.nsf/0/F677BFA978E00C938525714E0059D49C?Open&Highlight=0,global

permanent injunction, Global ceased operations and the individuals vowed to leave the phone record and pretexting business practice.¹⁶

The Consent Judgment and Permanent Injunction broadly provides that the following conduct is prohibited:

Defendants are permanently restrained and enjoined from making, or assisting others in making, expressly or by implication, any false or misleading oral or written statement or representation in connection with the marketing, advertising, promotion, offering for sale, sale or provision of any products or services in any trade or commerce, as follows (directly from the Judgment¹⁷):

- A. Initiating, assisting, facilitating, procuring, obtaining, or engaging, directly or indirectly, in any act or further attempts to obtain customer information including, but not limited to, calling or billing records, from any “telephone company” (as defined in paragraph 3.4 of this Section III) doing business in Florida through use of a telephone company customer’s “personal identification information”(as defined in paragraph 3.4 of this Section III);
- B. Directly or indirectly using any telephone company employee’s “identity” (as defined in paragraph 3.4 of this Section III) or purported identity for any purpose, specifically including any representation that one is a telephone company employee, agent or independent contractor;
- C. Directly or indirectly using any consumer or public utility

¹⁶ As a criminal investigation is underway, the Attorney General or his representative may be unable to address certain inquiries to avoid compromising the ongoing investigation.

¹⁷ The term “telephone company” is defined to specifically include Voice Over Internet Protocol (VoIP) and similar technological advancements; “Personal identification information” is defined to include the statutorily defined categories of information in section 817.568(1), such as telephone number, date of birth, etc; “Identity” is defined to include, *inter alia*, employer issued identification and individual access codes for computer interaction with accounts.

Certain language introducing the prohibited conduct has been paraphrased, and the foregoing definitions are paraphrased for convenience, but does not constitute an interpretation contrary to the Consent Judgment and Permanent Injunction entered by the court or an interpretation for substantive purposes as may be required at some future date.

customer's identity or purported identity for any purpose, specifically including any representation that one is a person other than himself;

- D. Directly or indirectly using any identity of a person or a business or purported identity for any purpose, specifically including any representation, through any means, that one is a person other than himself or maintains a telephone number other than his own number;
- E. Directly or indirectly making, or assisting others in making, expressly or by implication, any false or misleading oral or written statement or representation, intentional false statement, misrepresentation or omission of a material fact to induce reliance on such statement or omission with intent to use personal identification information of consumers without their knowledge or consent;
- F. Initiating, assisting, facilitating, procuring, or engaging, directly or indirectly, in any further contact with the customer service centers of any telephone company doing business in the State of Florida pertaining to any matter that is not directly related to Defendant's own account(s);
- G. Selling, transferring or disclosing to third parties any consumer information, including personal identification information and telephone calling records obtained from telephone companies, currently in Defendants' possession or under their control;
- H. Using confidential consumer information, including personal identification information and telephone calling records obtained from telephone companies, contained in any documents, regardless of form or manner of storage for marketing or for purposes inconsistent with the terms of this Judgment;
- I. Initiating, assisting, facilitating, participating, procuring, or engaging in any transaction with any other person or entity engaging in or performing in any of the activities prohibited by each of the paragraphs A. through G. of this Section III, paragraph 3.1.; and

- J. Forming, controlling, operating or participating in the control, operation or formation of a business or organizational identity as a method of avoiding the terms and conditions of this Judgment.

III. Florida Legislation and Existing Laws

A. Florida's New Law: Effective July 1, 2006:

Obtaining Telephone Calling Records by Fraudulent Means Prohibited as a Criminal Act

Florida has specifically criminalized the obtaining of telephone calling records through fraudulent means from a telecommunications company, as a bill unanimously approved by the Florida Legislature was signed into law on Friday, June 9, 2006 by Governor Jeb Bush.¹⁸

The new law will be inserted in Chapter 817, Fraudulent Practices, and will be located at Section 817.484, Fla. Stat. The content, in pertinent part, provides:

It is unlawful for a person to –

- (a) Obtain or attempt to obtain the calling record of another person without the permission of that person by:
1. Making a false, fictitious or fraudulent statement or representation to an officer, employee, or agent of a telecommunications company;
 2. Making a false, fictitious or fraudulent statement or representation to a customer of a telecommunications company; or

¹⁸ 2006-141, Laws of Florida, codified HB 871.

3. Providing any document to an officer, employee, or agent of a telecommunications company, knowing that the document is forged, is counterfeit, was lost or stolen, was fraudulently obtained, or containing a false, fictitious, or fraudulent statement or representation.

(b) Ask another person to obtain a calling record knowing that the other person will obtain, or attempt to obtain, the calling record from the telecommunications company in any manner described in paragraph (a).

(c) Sell or offer to sell a calling record that was obtained in any manner described in paragraph (a).

Violation of this law carries a 1st degree misdemeanor charge for a first offense resulting in sentencing up to a year imprisonment and up to \$1,000, but a second or subsequent offense imposes the heightened charge of a 3rd degree felony, resulting in a sentence of up to 5 years imprisonment and up to \$5,000.

Law enforcement agencies are exempt from the provisions of the new law; but an exemption for private investigators was eliminated in the legislative process.¹⁹ As private investigators appear to have played significant roles in the procurement of consumers' private information through unlawful means, they are clearly subject to the new law.

B. Florida's Existing Criminal Use of Personal Identification Information law

Existing law including, but not limited to, Section 817.568, Fla. Stat., addresses the fraudulent conduct encompassing pretexting and other identity theft related conduct, as set forth in the Attorney General's complaints and by the Consent Judgment entered in the Global litigation.

¹⁹ House of Representatives Staff Analysis dated April 10, 2006 (noting Justice Council Amendment removing exceptions contained in the original bill including activities of private investigators)
<http://www.flsenate.gov>

<http://www.flhouse.gov/Sections/Documents/loadoc.aspx?FileName=h0871d.JC.doc&DocumentType=Analysis&BillNumber=0871&Session=2006>

The foregoing specific laws are merely illustrative of one or more specific laws applicable to such unlawful conduct and other criminal and civil laws may apply given the circumstances of a particular course of conduct.

IV. Federal Communications Commission Rulemaking Authority and Telecommunications Carriers Should Enhance Telecommunications Carrier Protection of Private Consumer Information

Florida and forty-seven other state Attorneys General submitted comments to the Federal Communications Commission (“FCC”) on April 28, 2006, in response to the agency’s Notice of Proposed Rulemaking²⁰ to strongly encourage enhanced protections for consumers based on the ample experience of the Attorneys General in addressing consumer protection issues and employing enforcement measures.²¹ The discussion relates to telecommunications providers (“carriers”) disclosure and protection of Customer Proprietary Network Information (“CPNI”), more generally described as sensitive personal information, including logs of calls made and received by telephone customers.

Minimizing the security risks facing consumers, whose information is released to those skilled in deception, is an important focus for telecommunications carriers, regulators and legislators at the federal and state levels. Front-end protections created and implemented by carriers can prevent pretexters from plying their trade at the outset and eliminate investigative and prosecutorial functions deployed after the harm has occurred and the evidentiary trail compromised or obfuscated and impeded by the fact that a consumer may not even be able to

²⁰ RM-11277 relating to Telecommunications Carriers Use of Customer Proprietary Network Information (CPNI), CC Docket No. 96-115 (FCC NPRM)

²¹ The referenced comments submitted by the Attorneys General are available electronically at : <http://www.naag.org/news/pdf/20060509-FinalCPNICommentstoFCC.pdf>. The comments address, generally: enhanced security and authentication standards; existing privacy protections of CPNI; effectiveness of notices to customers regarding use of CPNI; extension of CPNI requirements to VoIP providers; wireless customers’ privacy expectations; adequacy of existing protections for privacy of CPNI; and the States recommendations.

identify that a compromise of their personal information has occurred. Deployment and implementation of heightened front-end consumer protections by telecommunications carriers as well as prosecutorial zeal are critical in stemming the tide of this industry. Prosecutorial resources require prudent use to keep all consumers safe from physical and economic harm. However, it is also fair and just that a substantial burden be shouldered by telecommunications carriers and all businesses subject to vulnerability through pretexting or other fraudulent conduct.

Why is immediate access to telephone records necessary? This is the real issue underlying access to consumer phone records. Consumers need to have a choice about access to their confidential records. Telecommunications carriers should voluntarily provide consumers with this critical choice. Should carriers fail to voluntarily provide consumers with an ability to exercise an informed choice, appropriate regulatory rulemaking or legislative action may become necessary. For example, if a consumer does not desire to access their records in an expedited manner such as by phone, fax or e-mail, they should be able to require the carrier to secure them appropriately. Alternatively, consumers desiring to obtain expedited access to their records could direct the carrier to permit internet or other access with appropriate checks and balances. Therefore, only those consumers willing to accept the inherent risks are subjected to increased vulnerability that a third party posing as a consumer might be able to access their records.

Akin to imposition of a security freeze on a credit report²² to protect unauthorized access or placement of a fraud alert on a credit report if one suspects identity theft, consumers must have a say in whether their confidential telephone records should be closed or be kept available for access by the consumer.

²² A security freeze will be an available option for Floridians effective July 1, 2006 as Governor Bush signed HB37 into law on June 9, 2006. 2006-124, Laws of Florida, codifies HB37.

The recommendations of the Attorneys General to the FCC warrant brief reiteration here for further emphasis and consideration of the responsibilities of telecommunications carriers:

1. Require Consumer Consent: Prior to a carrier's use, disclosure, or permitting access to a consumer's personal telephone records, consumers need to "opt-in" with affirmative express consent to permit their records to be accessed. While the comments address access to records for marketing, the next step in protecting disclosure of consumer records even outside of marketing is to require consumer consent to release the records in an expedited manner, as articulated above.
2. Bolster "safeguard rules" to adequately protect the confidentiality of consumer information. While Florida and many states have enacted security breach notification laws, a breach of security mechanisms through fraud may not invoke the notification provisions of the laws and consumers will not be alerted to review their personal accounts for theft or other wrongdoing.
3. Provide for revamp of consumer notices to permit informed consumers to make a choice about their personal information.
4. Extend requirements imposed on traditional telecommunications carriers to VoIP providers or Voice over Internet Protocol type technology. Florida's new law specifically provided for this technology.
5. Release of cell phone location should be treated cautiously to further safety concerns.
6. Engage in further review of the Safeguard Rule promulgated by the Federal Trade Commission in furtherance of the protections imposed on financial institutions,

particularly information security as it relates to (a) employee management and training; (b) information systems; and (c) managing system failures.

V. Vulnerability of Consumer Records Requires Evolving Strategies

Telephone records cases, including Global and others active in the consumer information industry, illustrate that the security of private consumer information beyond telephone records is at risk. Responsible corporate citizens and responsible consumers all have a role in protecting information from fraud and security vulnerabilities. Through responsible business practices, consumer education, regulatory oversight, as appropriate, and carefully considered legislation, the services sector and the consumer sector of the economy can meld to adjust to the changing world of consumer data. Federal legislation, however, should not impede any action by the states, pursuant to state law remedies. Congress, the FCC, state Legislatures and Public Service Commissions, and numerous others have taken positive steps to assess appropriate actions necessary to facilitate the process of positive change, as a cohesive approach will best serve all in the long run.

On behalf of Attorney General Charlie Crist, I appreciate the opportunity to participate in this hearing to address these important consumer protection issues and will respond to any further questions of the Subcommittee.